Keep Your Wearable Close, but Your Data Closer

Hari Sundaram
University of Illinois at Urbana Champaign
Urbana, IL, USA
hs1@illinois.edu

Robin Kravets
University of Illinois at Urbana Champaign
Urbana, IL, USA
rhk@illinois.edu

ABSTRACT

We have struck a Faustian bargain with major corporations—free information services in exchange for our web surfing behavioral data. Unfortunately, we have little control over not only what data is gathered about us, but also how long the data is stored and is used. Indeed, with the web, it is hard, if not impossible to be forgotten. As users interact with an Internet of Things (IoT) ecosystem, they leave behind traces of information about their presence, preferences and behavior. While the ecosystem can track individuals' movements to provide enhanced recommendations, individuals as with entities that track their web behavior, have little control over how this information is being used or distributed. Must the bargain between individuals and entities interested in tracking them in IoT environments, be asymmetric?

In response, we present Incognito, a secure and privacy preserving IoT framework where user information exposure is driven by the concept of identity. In particular, we advocate user-managed identities, leaving the control of the choice of identity in a given context, as well as the level of exposure, in the hands of the user. Using Incognito, users can create identities that work only within certain contexts and are meaningless outside of these contexts. Furthermore, Incognito allows for simple management of information exposure through contextual-policies for sharing as well as querying of an IoT ecosystem. By giving individuals full control over the information traces that they leave behind in an IoT infrastructure, Incognito, in essence, puts individuals on equal footing with the entities that want to track their behavioral data. Incognito fosters a symbiotic relationship; users will need to expose information in exchange for personalized recommendations and IoT organizations who provide sophisticated user experiences will see enhanced user engagement.

ACM Classification Keywords

K.4.1 Public Policy Issues: Privacy; C.2.1 Network Architecture and Design: Wireless communication

Author Keywords

IoT, Privacy

INTRODUCTION

By the time you are finished surfing the web for the day, several hundred entities using third-party cookies would have tracked your movements over the web [6]. This information would then be aggregated, and traded over real-time exchanges, with much of this activity occurring without your informed consent. While many websites let visitors know that they use third-party cookies, individuals have very little idea about the extent of information that is gathered about them by third-party tracking entities and are unable to query entities about what is stored about them.

We seem to have struck a Faustian bargain with major corporations—tracking of behavioral data in return for free information services—and where the corporations are largely driven by advertising revenue. It is an asymmetric bargain—not only are individuals unable to determine what information is stored about them, but also they are largely powerless to prevent tracking and to control use of their behavioral data. Furthermore, this stored information may also be used in unexpected ways, for example to assess your credit history [1].

With the emergence of connected infrastructures, the Internet of Things (IoT), our physical world behavior will likely be tracked with the same precision and granularity as our web surfing behavior. Must the bargain between individuals and corporations remain asymmetric in the context of IoT? In this abstract, we present we discuss Incognito, a protocol that allows individuals to be in full control of their information exposure. Incognito helps create a symmetric relationship between individuals and corporations interested in tracking them and which builds upon our recent work on IoT privacy [2]. We argue that in the context of IoT, if the control of a user's data is entirely left to external organizations, users will remain skeptical and likely forgo the use of any IoT ecosystem, limiting the benefits to all parties involved.

Every day, users are interacting with hundreds and thousands of devices in both intentional and unintentional ways. Currently, these devices are being linked through local and cloud services to form an Internet of Things. As users interact with this IoT in stores, museums and other public spaces to find useful localized information, they leave breadcrumbs in the form of information traces about their presence, preferences and behavior. By intentionally exposing pieces of their personal information, users could benefit from complex services and enhanced interactions. Additionally, organizations, including retail locations and museums, can provide sophisticated benefits in exchange for this information. However, to prevent unintentional leaks of personal information, users must be able to manage their information exposure. To this end, the users and organizations need to collaborate through an IoT ecosystem that benefits both the users and organizations, while allowing the users to protect their personal information.

To achieve the full potential of such an IoT ecosystem, the breadcrumbs collected in an environment must be associated with a user. As more and more information is collected about a user, more and more refined recommendations can be made. By tracking individuals and their data, the information in their individual data traces can be aggregated into meaningful business intelligence, allowing users, companies and organizations to leverage the vast potential of IoT. The benefits of exposing user information and interacting locally with the physical entities in a user's environment, as well as the IoT ecosystem as a whole, can be immense. These benefits can range from simple scenarios that improve a user's tour of a museum (*e.g.*, "What did other people with an interest in impressionism see here?") or shopping experience in a grocery store (*e.g.*, "What do other people who are on a diet buy here?"), to more complex scenarios that can help a user navigate through a foreign city (*e.g.*, "What did my parents order when they visited this café?"; "What do locals like to do?"). Additionally, by allowing users to query the IoT ecosystem, they can look back at their own traces to see what they have done in the past. To benefit from any of these examples, users must be willing to expose some amount of information about themselves to help provide personalized recommendations.

However, as new technologies are deployed, users are still unsure of how to interact with the world around them, or if they even want to. Even though users are afraid of exposing too much personal information, it is clear that they are willing to expose some information if they receive concrete benefits (*e.g.*, EZpass provides faster and discounted road toll payments, frequent buyer supermarket apps give fuel discounts and free food). Although we are already seeing many new applications in this direction, there is an all or nothing approach to information exposure. Instead of exposing their identity all of the time, when shopping, a user may only want to expose that they are vegetarian to help them navigate through a store. By exposing a little more information about their identity and shopping history, the user may be given new suggestions for what to buy or even access to special sales. However, a user may not want to expose all of their personal information in a given context. They may even want to go so far as to interact anonymously.

Contemporary culture, with dystopian visions of a future where individuals seamlessly interact with the physical world around them (*e.g.*, the film "Minority Report") mirrors individual's fears of information exposure. In a typical scenario, powerful corporations and government agencies track individuals as they interact with their environment. Although these visions of the future are very off-putting to many users, they are not so far from the current capabilities of data aggregators. Indeed these capabilities, including the user's security concerns have started to raise concerns about IoT with policy makers [4, 5].

In response, we envision a radically different future where individuals are in full control of their information exposure, including traces that they leave behind with any part of the IoT ecosystem. In particular, in exchange for intentional exposure of limited information, individuals can access unique, complex services, beyond product recommendations or advertisements. However, currently, there is no simple way for a user to manage their exposure and how the exposed information is re-used. In this abstract, we discuss the design of Incognito, a framework where user information exposure is driven by the concept of identity. When interacting with the IoT ecosystem using Incognito, individuals, not the ecosystem, are in control of the "identity" they expose. By giving individuals full control over the information traces that they leave behind in an IoT infrastructure, Incognito, in essence, puts individuals on equal footing with the entities that want to track their behavioral data. While identity is currently being addressed in IoT systems, the main focus is the identity of the things [3], not of the users.

To enable flexible management of user information, Incognito allows each user to generate multiple identities or pseudonyms, based on their context—location, domains, personal state, and time—that we term *contextual identity*. (`cid`). For example, the user could have one identity for each store they visit, or a new identity for each time they visit a store. The user can then limit information exposure and aggregation by managing access to their breadcrumbs on a per-identity basis. Additionally, if they want to disconnect from one of their identities, they simply stop using it and create a new identity, thus enabling a limited form of "digital forgetting."

Essentially, each user controls how much information is passed on, and so potentially stored and used for recommendations, by the ecosystem by setting location- and app-specific identities inside Incognito. Incognito manages all communication with the IoT ecosystem, eliminating information leaks to the apps running on a user's mobile device. Furthermore, with Incognito, an individual's data stored in the IoT ecosystem is available to that person via an authenticated query, as well as to friends to whom the individual has granted access. Given the increasing concern over the use by advertisers of third-party cookies to track individuals' web-browsing [6], we believe that putting control of a user's information exposure in the hands of the user is critical to widespread adoption of IoT by the public.

REFERENCES

1. Lori Andrews. 2012. Facebook Is Using You. The New York Times. (Feb 2012). http://nyti.ms/1GGOG46.
2. Robin Kravets, Güliz Seray Tuncay, and Hari Sundaram. 2015. For Your Eyes Only. In *Proceedings of the 6th International Workshop on Mobile Cloud Computing and Services*. ACM, 28–35.
3. David Meyer. 2014. Samsung invests in internet of things identity management platform Evrythng. (Oct. 2014). http://bit.ly/1JoTivU.
4. Natasha Singer. 2015. F.T.C. Says Internet-Connected Devices Pose Big Risks. The New York Times. (Jan 2015). http://nyti.ms/1MPWgby.

5. The Economist. 2014. The internet of things (to be hacked). (July 2014). http://econ.st/1FQ3A1Y.

6. Joseph Turow. 2012. *The daily you: How the new advertising industry is defining your identity and your worth*. Yale University Press.